Amendments to the Claims:

This listing of claims will replace all prior versions and listings of claims in the application. Please amend the claims as follows:

Listing of Claims:

1. (Currently Amended) In an initiating system, a computer-implemented method for establishing a new group identity, the method comprising:

~~creating group identity information;~~

receiving a selection ~~selecting a first subset~~ of [[the]] group identity information for a first group to include in a first group identity information document for disclosure to a first receiving system;

~~selecting a second subset of the group identity information to include in a second group identity information document for disclosure to a second receiving system, wherein the second subset is different from the first subset, and wherein the second receiving system is different from the first receiving system;~~

generating a first group-signed group identity information document comprising the ~~first subset of the~~ group identity information for the first group, an embedded use policy that expresses a privacy policy providing instructions as to how the ~~first subset of the~~ group identity information for the first group may be used, wherein the embedded use policy is stored with the ~~first subset of the~~ group identity information for the first group, at least a first key, and a first group identity information document signature signed by [[a]] an ~~group~~ owner of the first group using a second key associated with the first key, wherein the second key is a private key of the first group and is owned by the first group owner;

sending the first group-signed group identity information document to the first receiving system to establish the first group as a new group identity at the first receiving system;

receiving a selection of personal identity information to include in a personal certificate for an originator;

generating a self-signed personal certificate using the selection of personal identity information, wherein the self-signed personal certificate establishes the originator's personal identity, and wherein the self-signed personal certificate is signed by the originator;

attaching the self-signed personal certificate to a first message for sending to the first receiving system;

determining whether to attach, to the first message, a first group-signed membership certificate with the self-signed personal certificate, wherein the first group-signed membership certificate is group-signed by the first group owner, and wherein the first group-signed membership certificate establishes the originator's membership identity in the first group;

when the first group-signed membership certificate is to be attached to the first message:

attaching the first group-signed membership certificate with the self-signed personal certificate to the first message for sending to the first receiving system;

determining whether to attach, to the first message, an additional membership certificate with the first group-signed membership certificate and the self-signed personal certificate; and

when no additional membership certificate is to be attached, sending the first message with the attached self-signed personal certificate and the attached first group-signed membership certificate to the first receiving system.

2. (Cancelled)

3. (Cancelled)

4. (Cancelled)

5. (Cancelled)

6. (Cancelled)

7. (Cancelled)

8. (Currently Amended) The method of claim [[6]] 1 further comprising:

receiving, at the first receiving system, the first group-signed membership certificate ~~identity information document~~ and the self-signed personal certificate ~~identity information document~~ from the originator;

detecting whether the new group associated with the first group-signed membership certificate ~~identity information document is~~ has been previously accepted and whether the originator ~~person~~ associated with the self-signed personal certificate ~~identity information document is~~ has been previously accepted;

assigning a first security protocol based on a security protocol for the first group ~~protocols~~ to communications from the originator [[if]] when the new group [[is]] has been previously accepted; and

assigning a second security protocol based on the personal identity of the originator ~~protocols~~ to communications from the originator [[if]] when the personal certificate has been previously ~~person is~~ accepted.

9. (Currently Amended) In a communication system, an apparatus for establishing a new group identity of a first group at a first receiving system, comprising:

an initiating system, comprising a processing unit and computer storage media, the computer storage media encoding modules for execution by the processing unit, including:

a group ID generate module generating a first group-signed group certificate comprising at least a public key, a digital signature for the first group, and an embedded

use policy that expresses a privacy policy providing instructions as to how a first subset of group identity information for the first group may be used at [[a]] the first receiving system, wherein the embedded use policy is stored with the first subset of group identity information for the first group, and wherein the first subset of group identity information is selected from group identity information for disclosure to the first receiving system ~~and a second subset of group identity information is selected from the group identity information for disclosure to a second receiving system, the first subset being different from the second subset~~; [[and]]

a send module transmitting the group certificate to the first receiving system to establish the new group identity of the first group at the first receiving system;

a receive module for receiving a selection of personal identity information to include in a personal certificate for an originator;

a personal ID generate module for generating a self-signed personal certificate using the selection of personal identity information, wherein the self-signed personal certificate establishes the originator's personal identity, and wherein the self-signed personal certificate is signed by the originator;

an attach module for attaching the self-signed personal certificate to a first message for sending to the first receiving system;

a determination module for determining whether to attach, to the first message, a first group-signed membership certificate with the self-signed personal certificate, wherein the first membership certificate is group-signed by the first group owner, and wherein the first group-signed membership certificate establishes the originator's membership identity in the first group;

when the first group-signed membership certificate is to be attached to the first message:

the attach module attaching the first group-signed membership certificate with the self-signed personal certificate to the first message for sending to the first receiving system;

the determination module determining whether to attach, to the first message, an additional membership certificate with the first group-signed membership certificate and the self-signed personal certificate; and

when no additional membership certificate is to be attached, the send module sending the first message with the self-signed personal certificate and the first group-signed membership certificate to the first receiving system.

10. (Cancelled)

11. (Currently Amended) The apparatus of claim [[10]] 9 further comprising:

a membership ID generate module for generating the first group-signed [[a]] membership certificate having at least a public key ~~of the sender~~ and a digital signature for the new group;

a save module, responsive to the membership ID generate module, storing the first group-signed membership certificate;

a retrieve module retrieving the first group-signed membership certificate from the save module and providing the first group-signed membership certificate to the attach module.

12. (Currently Amended) The apparatus of claim [[10]] 9 further comprising:

[[a]] the first receiving system[[,]] comprising a processing unit and computer storage media, the computer storage media encoding modules for execution by the processing unit, including:

a receive module at the first receiving system receiving the first group-signed membership certificate; and

an accept module at the first receiving system detecting whether to accept the first group-signed membership certificate.

13. (Currently Amended) The apparatus of claim 12 further comprising:

an assign module, at the first receiving system, assigning a security identification to communications from the ~~sender~~ originator based on the new group associated with the first group-signed membership certificate [[if]] when the first group-signed membership certificate is accepted by the accept module.

14. (Cancelled)

15. (Currently Amended) The apparatus of claim [[12]] 9 further comprising:

~~a personal ID generate module generating a personal certificate having at least a public key of the sender and a digital signature by the sender;~~

a receive module at the first receiving system receiving the certificates;

an accept module at the first receiving system detecting if the certificates are to be accepted;

an assign module, at the first receiving system, assigning a first security protocol to communications from the originator ~~sender~~ based on [[a]] the group identity of the first group associated with the first group-signed membership certificate [[if]] when the first group-signed membership certificate is accepted by the accept module;

~~the send module transmitting the personal certificate to establish the sender's identity at the first receiving system; and~~

the assign module, at the first receiving system, assigning a second security protocol to communications from the originator ~~sender~~ based on the personal identity associated with the self-signed personal certificate [[if]] when the self-signed personal certificate is accepted by the accept module at the first receiving system.

16. (Currently Amended) A computer storage medium readable by a computing system and encoding a computer program of instructions for executing a computer process for establishing a new group identity in communications between an initiating system and a first receiving system, said computer process comprising:

generating, at the initiating system, a first group-signed group certificate comprising at least an embedded group use policy that expresses a privacy policy providing instructions as to how a first subset of group identity information for a first group may be used at the first receiving system, wherein the embedded use policy is stored with the first subset of group identity information for the first group, a group public key and a digital signature for the group signed, by a group owner of the first group, with a group private key associated with the group public key, and wherein the first subset of group identity information for the first group is selected from group identity information for disclosure to the first receiving system ~~and a second subset of group identity information is selected from the group identity information for disclosure to a second receiving system, the first subset being different from the second subset~~;

sending the first group-signed group certificate to the first receiving system to establish the first group as a new group identity at the first receiving system;

receiving a selection of personal identity information to include in a personal certificate for an originator;

generating a self-signed personal certificate using the selection of personal identity information, wherein the self-signed personal certificate establishes the originator's personal identity, and wherein the self-signed personal certificate has at least a public key of the originator, an embedded personal use policy that expresses a personal privacy policy providing instructions as to how personal identity information may be used, wherein the embedded personal use policy is stored with the personal identity information, and a digital signature using the private key of the originator;

attaching the self-signed personal certificate to a first message for sending to the first receiving system;

determining whether to attach, to the first message, a first group-signed membership certificate with the self-signed personal certificate, wherein the first group-signed membership certificate is group-signed by the first group owner, and wherein the first group-signed membership certificate establishes the originator's membership identity in the first group;

when the first group-signed membership certificate is to be attached to the first message:

attaching the first group-signed membership certificate with the self-signed personal certificate to the first message for sending to the first receiving system;

determining whether to attach, to the first message, an additional membership certificate with the first group-signed membership certificate and the self-signed personal certificate; and

when no additional membership certificate is to be attached, sending the first message with the self-signed personal certificate and the first group-signed membership certificate to the first receiving system

~~sending a membership certificate to the first receiving system to establish an originator as a member of the new group at the first receiving system;~~

~~generating a personal certificate having at least a public key of the originator, a personal use policy that expresses a personal privacy policy providing instructions as to how personal identity information may be used, wherein the embedded personal use policy is stored with the personal identity information, and a digital signature for the originator signed by the originator with a private key associated with the public key of the originator; and~~

~~sending the personal certificate to establish the personal identity of the originator at the first receiving system~~.

17. (Cancelled)

18. (Currently Amended) The computer ~~readable~~ storage medium of claim 16 wherein the process further comprises:

creating the first group-signed membership certificate at the initiating system~~, the membership certificate having at least a public key of the originator and a digital signature signed using the group private key~~.

19. (Currently Amended) The computer ~~readable~~ storage medium of claim 16 wherein the process further comprises:

receiving the first group-signed membership certificate at the first receiving system; and

testing acceptance of the group identity of the first group received in the first group-signed membership certificate.

20. (Currently Amended) The computer ~~readable~~ storage medium of claim 19 wherein the process further comprises:

assigning a first security protocol to communications from the originator based on the new group identity of the first group [[if]] when the first group-signed membership certificate is accepted by the act of testing.

21. (Cancelled)

22. (Currently Amended) The computer ~~readable~~ storage medium of claim 16 wherein the process further comprises:

accepting the identity information in the certificates received at the first receiving system [[if]] when the certificates have been previously accepted;

assigning a first security identification to reflect a security protocol for [[to]] communications from the originator, wherein the first security protocol is applied to communications for the first group ~~based on the first subset of group identity information if the membership certificate is accepted~~; and

assigning a second security identification to reflect a second security protocol for communications from the originator, wherein the second security protocol is applied to communications from the originator based on the personal identity of the originator ~~based on the personal identity information of the originator if the personal certificate is accepted~~.